CLAIMS:

What is claimed is:

1. A method of testing a device comprising:

providing a first data string;

providing a second data string in a memory structure;

encrypting the first data string using an encryption algorithm, to provide an encrypted data string; and

comparing a characteristic of the encrypted data string with a characteristic of the second data string.

2. The method of claim 1 wherein the step of comparing a characteristic of the encrypted data string with a characteristic of the second data string comprises comparing the bit length of the encrypted data string with the bit length of the second data string.

3. The method of claim 2 and further comprising, if a match is found between the bit length of the encrypted data string and the bit length of the second data string in the memory structure, comparing an initialization vector associated the encrypted data string with an initialization vector applied in encrypting the first data string.

4. The method of claim 3 and further comprising, if a match is found between the initialization vector associated with the encrypted data string and the initialization vector applied in encrypting the first data string:

extracting the initialization vector associated with the encrypted data string;

applying the encryption algorithm to the second data string, using the extracted initialization vector, to provide an additional encrypted data string;

comparing contents of the additional encrypted data string with contents of the previously generated encrypted data string.

5. The method of claim 1 wherein the data string in the memory structure is an unencrypted data string.

6. A method of testing a device comprising:

providing a first data string;

providing a second data string in a memory structure;

encrypting the first data string using an encryption algorithm, with an initialization vector applied in such encryption, to generate an encrypted data string; and

comparing an initialization vector associated with the encrypted data string with the initialization vector applied in encrypting the first data string.

7. A method of testing a device comprising:

providing a first data string;

providing a plurality of data strings in a memory structure;

encrypting the first data string using an encryption algorithm, with an initialization vector applied in such encryption, to generate an encrypted data string; and

comparing the initialization vector associated with the encrypted data string with the initialization vector applied in encrypting the first data string.

8. The method of claim 8 wherein the step of comparing a characteristic of the encrypted data string with a characteristic of a data string in the memory structure comprises comparing the bit length of the encrypted data string with the bit length of a data string in the memory structure.

9. The method of claims 8 and further comprising, if a match is not found between the bit length of the encrypted data string and the bit length of a data string in the memory structure, comparing the bit length of the encrypted data string with the bit length of another data string in the memory structure.

10. The method of claim 8 and further comprising, if a match is found between the bit length of the encrypted data string and the bit length of a data string in the memory structure, comparing an initialization vector associated with the encrypted data string with the initialization vector applied to the encryption engine.

11. The method of claim 10 and further comprising, if a match is found between the initialization vector in the encrypted data string and the initialization vector applied in the encryption of the first data string;

extracting the initialization vector associated with the encrypted data string;

applying the encryption algorithm to the matching length data string from the memory structure to provide an additional encrypted data string; and

comparing contents of the additional encrypted data string with contents of the previously provided encrypted data string.

12. The method of claim 11 wherein the data strings in the memory structure are unencrypted data strings.